UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/838,979	04/19/2001	Peter V. Radatti	E-2532	1266

7590 01/09/2008

John F.A. Earley III
86 The Commons at Valley Forge East
1288 Valley Forge Road
P.O. Box 750
Valley Forge, PA 19482-0750

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
01/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>22 October 2007</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☒ Claim(s) *14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 10/22/07. The amendment filed

on 10/22/07 have been entered and made of record. Therefore, presently pending claims are 1-

14.

Response to Arguments

Applicant's arguments filed 10/22/07 have been fully considered but they are not

persuasive because of following reasons.

Applicant argued that the evaluated writing of the interpreted code is what is provided as

the result which is scanned for the presence of proscribed code. This is not found persuasive. As

shown in Fig. 5 of the Nachenberg reference, the system executes P-code (part 510) and

emulation (part 516) and further sent to scan process. In the system the result of the emulation

and execution is the file itself. This file is then sent to the scanned (part 526).

The applicant argues further that Nachenberg discloses scanning the suspect file itself.

This is found persuasive. The file disclosed by Nachenberg corresponds to the result of the

application.

The applicant argues further that the interpreted results are evaluated and analyzed and

are not emulated. This is not found persuasive. As disclosed in the Fig. 5, the results, file, are

processed through several steps. The application does not prohibit other processes being

performed on the results before the scanning occurs.

The examiner asserts that Nachenberg does teach or suggest the subject matter broadly

recited in independent Claims. Dependent Claims are also rejected at least by virtue of their

dependency on independent claims and by other reason set forth in this office action.

Accordingly, rejections for claims 1 are respectfully maintained.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
requirements of this title.

Claims 7-14 rejected under 35 U.S.C. 101 because the claimed invention is directed to

non-statutory subject matter. The claims as recited do not produce a final tangible result.

Instead the claims disclose an algorithm that has a final result of reporting the results to a results

evaluator and from the results evaluator to a reporter. There is no tangible result.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
patent by another filed in the United States before the invention by the applicant for patent, except that an
international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
subsection of an application filed in the United States only if the international application designated the United
States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 6 and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by

Nachenberg (6,851,057).

In reference to claims 1, 6, and 13, Nachenberg discloses a virus detection system that operates under the control of P-code to detect the presence of a virus in a file having multiple entry points (abstract). The method of virus detection includes interpreting code with an interpreter (column 7 lines 35-40); evaluatively writing with said interpreter the result of said interpretation (column 7 lines 60-65), wherein the interpreter evaluates the P-code in the P-code data file and writes to the data file; and scanning the results of said interpretation for the presence of proscribed code and identifying proscribed code in said results (column 7 line 66 to column 8 line 5), and making results available to a reporter for reporting (column 3 lines 64-67).

In reference to claim 2, wherein scanning the results of said interpretation for the presence of proscribed code further comprises scanning for the presence of code of interest. Nachenberg discloses scanning for virus signature and therefore for presence of code of interest (column 8 lines 1-2).

In reference to claim 3, wherein the first scanning step for the presence of code of interest further comprises scanning for a file open command or a file modify command (column 7 lines 45-67).

In reference to claim 4, Nachenberg discloses a method wherein scanning the results of the interpretation for the presence of proscribed code further comprises scanning for the presence of code of interest (column 7 lines 45-67 in combination with column 8 lines 1-5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 7-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg as applied to claim 1, and 4 respectfully above, and further in view of Shieh et al (5,278,901).

In reference to claim 7, is rejected as in claim 1 wherein Nachenberg discloses a virus detection system that operates under the control of P-code to detect the presence of a virus in a file having multiple entry points (abstract). The system includes an evaluative code interpreter (column 7 lines 35-65); a results evaluator (column 7 lines 66-67); a reporter (column 3 lines 64-66); whereby, after proscribed code is interpreted by said evaluative code interpreter and results generated, those results are reviewed for the presence of proscribed code (column 7 line 66 to column 8 line 5), and results reported to said results evaluator, and from said results evaluator to a reporter (column 9 lines 47-65).

However Nachenberg does not expressly disclose a pattern analyzer.

However Shieh discloses a pattern-oriented system and method of intrusion detection (column 4 lines 9-22). The pattern-oriented system is used to detect virus propagation (column 16 lines 31 to column 17 line 30); therefore the pattern analyzer reviews patterns for the presence of proscribed code.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add a pattern analyzer for detection for intrusion detection as in the system by Shieh in the system of Nachenberg. One of ordinary skill in the art would have been motivated

to do this because patterns are a simple way of defining deviation from the normal operation of

the system.

In reference to claim 5, Nachenberg does not expressly disclose a system wherein the

second scanning step for the presence of proscribed code of interest further comprises scanning

for viral code or viral patterns.

However Shieh discloses a pattern-oriented system and method of intrusion detection

(column 4 lines 9-22).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use pattern detection for intrusion detection as in the system by Shieh in the

system of Jordan. One of ordinary skill in the art would have been motivated to do this because

patterns are a simple way of defining deviation from the normal operation of the system..

In reference to claim 8, Nachenberg discloses a system wherein the step of scanning

further comprising a first scanning step for the presence of code of interest (column 8 lines 1-5).

In reference to claim 9, wherein the first scanning step for the presence of code of interest

further comprises scanning for a file open command or a file modify command (column 7 lines

46-64).

In reference to claims 10-12, Nachenberg does not expressly disclose the pattern analyzer

further reviews said code for the presence of code of interest.

Shieh discloses the pattern analyzer reviews code for the presence of problems, or code

of interest (column 4 line 60 to column 5 line 11).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use pattern detection for code of interest as in the system by Shieh in the system

of Jordan. One of ordinary skill in the art would have been motivated to do this because patterns

are a simple way of defining deviation from the normal operation of the system.

Allowable Subject Matter

Claim 14 is objected to as being dependent upon a rejected base claim, but would be

allowable if rewritten in independent form including all of the limitations of the base claim and

any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Thanhnga B. T

PWK
Monday, January 07, 2008

THANHNGA TRUONG
PRIMARY EXAMINER